2. Approach to IT Standards Guidance (ITSG)

This chapter provides the basis for the organization and selection of standards and guidance. The relationship of this chapter to the rest of the document is shown in Figure 2-1.

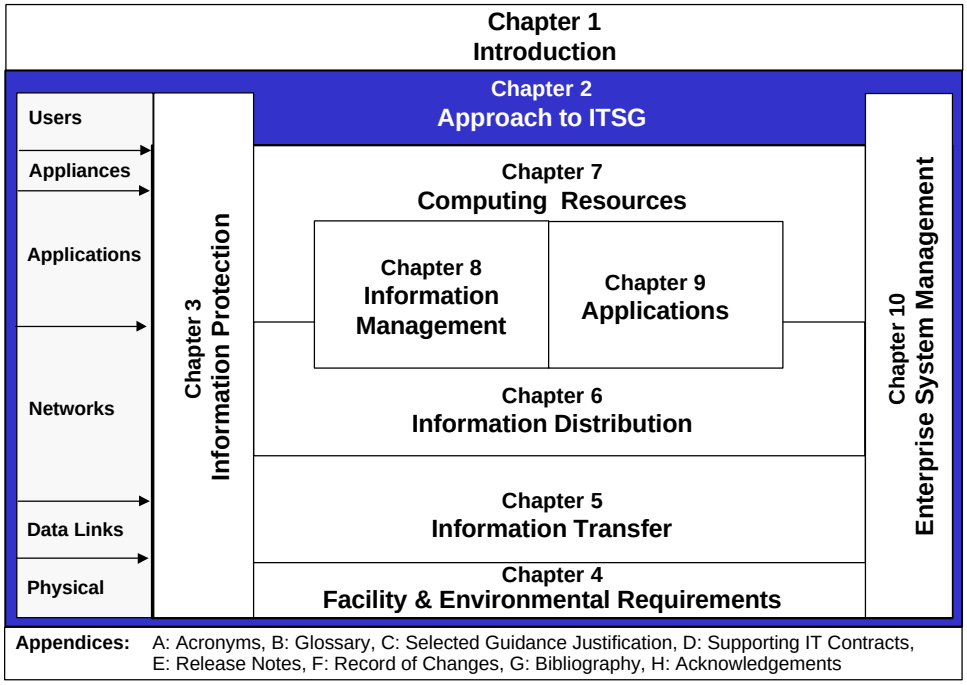

Figure 2-1. ITSG Document Map Highlighting Chapter 2, Approach to ITSG

The ITSG supports the Department of the Navy's migration from independent, application-based, stand-alone functional systems to a single enterprise information infrastructure – one that enables functional applications to be inserted and extracted as modules without disruption to the overall enterprise system. Equally important, it provides guidance to support refreshment of technology components that comprise the infrastructure itself. The ITSG is the guidebook for network-centric implementation to achieve information superiority.

The ITSG is not intended to be a shopping list of universally accepted standards that justify selections already made by program managers and system implementers, nor is it intended to be a restatement of existing documents such as the Joint Technical Architecture (JTA). It is intended to bound the options that systems implementers have so that they converge upon a common architecture and interoperability. The ITSG does provide enough tolerance, however, to allow introduction of emerging standards and selection of standards applicable to unique operational environments.

The ITSG attempts to completely cover all aspects of IT implementation and is organized so that the system developer, integrator and manager can quickly get to the information relevant to their mission. This is a challenging task because the universe of IT is vast, expanding, and moving. This chapter provides a description of the ITSG approach, organization and coverage.

The Navy and Marine Corps face the challenge of providing technologically advanced IT capabilities to the warrior and support forces while balancing these against the immaturity and uncertain market-acceptance of these same technologies. This is a special concern to network

designers as infrastructure costs are high and disruption/downtime during installation can be significant. To provide guidance to managers, integrators and designers, the goals of these standards are as follows:

- Promote national and international consensus from such bodies as the Internet Engineering Task Force (IETF), the ATM Forum, the American National Standards Institute (ANSI), the International Telecommunications Union (ITU) and others.
- Reduce the dependence on proprietary solutions.
- Offer the best potential for scalability, adaptability and market acceptance while minimizing the financial and loss-of-service consequences of choosing/replacing non-optimal components.
- Allow for controlled growth and upgrades as requirements change and expand.

2.1 Best Practices, Standards, Products and Guidance

Open system standards are embraced as the desired tenets for building the information infrastructure. Where such standards do not exist, the Department of the Navy (DON) ITSG will provide best practices or direction, if possible. When the state of the technology is not clear, the ITSG will provide as much guidance to the user as possible. Unlike the JTA and other standards documents, the ITSG is more of a guidance document so that the "strictness" of the definition of a standard does not interfere with its usefulness and timeliness in supporting the architecture. Simplified definitions of these guiding elements are provided below and are intended to put useful guiding principles, not limited to standards, in context. They offer perspective on how a guiding element applies to Information Technology (IT) development, integration, acquisition or operational implementation. The formal definition of these terms is provided in the glossary, Appendix B.

Policy. A standing set of general principles or guidelines on a topic deemed to be mandatory.

Guidance. Any statement of direction or recommendation, not necessarily mandatory.

Specification. A well defined, well described design, protocol, or practice.

Standard. A selected and approved specification or set of specifications by an authoritative body.

De facto standard. A specification or product that by its sheer market acceptance is considered to be the most suitable.

Best Practices. Practices that are considered to be the most effective and efficient.

Available Products. Products that meet the system requirement.

Preferred Products. Products that are deemed more suitable than others.

2.1.1 Open System Standards

An open system describes products and technologies that have been designed and implemented according to open interfaces. Interfaces are considered open if their specifications are readily available to all suppliers, service providers, and users, on a non-discriminatory basis. They are

revised only with timely notice and public process. The DON CIO also recognizes that openness is not truly achieved until multiple commercial companies adopt and implement those standards.

Several organizations have developed and continue to maintain standards for open systems. The DON ITSG Integrated Product Team (IPT) has examined the standards of these organizations while considering the joint requirements of the DOD, services (Navy, Marine Corps, Army, and Air Force), and other agencies. In order of preference for the standards presented, these organizations are as follows:

United States standards bodies – These organizations include American National Standards Institute (ANSI) and the National Institute for Standards and Technology (NIST).

International standards bodies – These standards organizations develop and maintain international standards:

International Organization for Standardization (also known as International Standards Organization [ISO]) – This body issues standards on numerous subjects ranging from hardware and software to information processing. ISO consists of the national standards organizations of more than 89 member nations.

International Telecommunications Union-Telecommunications Standardization Sector (ITU-T) (formerly named Consultative Committee on International Telephony and Telegraphy [CCITT]) – This body, responsible for worldwide telecommunications standards, makes technical recommendations about telephone, telegraph, and data communication interfaces. ITU-T is part of the United Nations treaty organization called International Telecommunications Union (ITU). ISO and ITU-T sometimes cooperate on issues of telecommunications standards. ISO is a member of ITU-T.

Internet Engineering Task Force (IETF) – The IETF, under the responsibility of the Internet Activities Board (IAB), publishes Requests for Comments (RFCs). The body of RFCs comprises a widely implemented set of Internet protocol suite standards. These standards are the basis for the strategic interconnection technologies of the public Internet

Institute of Electrical and Electronics Engineers (IEEE) – The IEEE sets standards for various communications and systems interfaces. IEEE defined Portable Operating System for Information Exchange (POSIX) standards that the U.S. government has adopted.

Industry Consortia – These consortia consist of end users, software suppliers, and computer manufacturers, and are international in scope and influence. Industry consortia considered in the DON ITSG include: The Open Group (TOG), which was created through the merger of X/Open and the Open Software Foundation (OSF), the Network Management Foundation (NMF), and the Asynchronous Transfer Mode (ATM) Forum, among others.

National standards bodies – It may be useful to follow standards from organizations. These organizations include British Standards Institution (BSI), French Association for Standardization (or Association Française de Normalisation [AFNOR]), German Industrial Standards Institute (or Deutsches Institut fur Normung [DIN]), and Japanese Industrial Standards Committee (JISC).

2.1.2 De Facto Standards

Even though open systems standards are embraced as the desired goal for the DON, de facto standards cannot be ignored and must be incorporated to some degree. Increasingly, de facto standards are becoming the industry determinant for technology evolution because the open systems process, by its very nature, will never move forward as rapidly as the de facto standards process. In some cases, de facto standards may be preferred over open standards that are not complete or not widely supported by available products. Additionally, de facto standards must be adopted because of wide use or acceptance. The ITSG IPT will incorporate prevalent de facto and industry consortia standards as appropriate.

2.1.3 Product Suite and Products

Where there is no standard, the ITSG will provide as much guidance as possible on the selection of product suites or products. Product suites or products will be embraced when current standards are insufficient to guarantee interoperability.

Information service providers must develop and integrate platform architectures using products from multiple suppliers. In many IT areas, competing standards and products provide little basis for selection. Here, the concept of working sets, or product suites, has gained popularity. Users can choose a collection of products and capabilities that promise to work well together to minimize the risk of incompatibilities among multiple-vendor products that are not built to work together. The cumulative advantages of a suite of products often outweighs the competitive advantages from using “open” products that have their unique “features”. The ITSG recognizes this and seeks to take advantage of these working set efficiencies

2.1.4 Order of Precedence

All things being equal, products that comply with open system standards are the preferred choice. Products that support de facto standards are the second choice. However, to perform a common function, the Navy and Marine Corps will not accept multiple, non-interoperable products. A single product suite or single product that tightly integrates multiple functions well is preferred over a federation of products, assuming there is an associated improvement in performance or price and guaranteed compliance with future open system management standards.

2.2 Application of Standards and Guidance

The specific use of standards and guidance varies depending upon the role of the IM/IT worker. A software engineer normally thinks of elements within a programming toolkit such as the Distributed Computing Environment (DCE). The system integrator thinks of interface standards such as Asynchronous Transfer Mode (ATM). The system user thinks of standard products such as Netscape. To organize these guiding elements, the ITSG places standards and guidance into three categories.

Development. How to program, design or develop a system component. Applicable to design engineers and software developers. Normally supports information processing.

System Integration. How to integrate system components into a system or system architecture. Applicable to system engineers and system architects. Supports end-to-end information flow.

Operational. What to use and/or how to configure and implement a system to maximize operational effectiveness. Applicable to process improvement. These are required for business and warfare process improvement.

2.3 Level of Abstraction

Like the application of standards and guidance, the associated level of detail also spans a range of needs. For example, the specific details of the International Telecommunications Union – Telecommunications (ITU-T) X.400 standard for electronic messaging is important to the developer of an electronic mail (e-mail) application. On a higher level of abstraction, the system engineer tracks the interface specifications of the standard to understand the compatibility between products as well as interoperability and translation requirements with other standards. The system engineer also understands other standards such as the Internet Engineering Task Force (IETF) Simple Mail Transfer Protocol (SMTP) standard and needs to select one standard over another to maximize system integration. At the greatest level of abstraction, the project manager understands the rationale for the selection of a particular standard such as SMTP over X.400 to guide system development and to identify products that support the messaging capability.

The three levels of abstraction are:

Technical. Highly precise and very detailed set of specifications that describe a standard or practice.

Integration. A more generalized description of standards — practices that reference technical specifications with specific application guidance.

Management. A description of the information system characteristics provided by a set of referenced standards or guidance and how it translates into total architecture capability.

The ITSG aims for the middle level of abstraction – integration, recognizing that a greater level of technical detail may be needed to ensure interoperability. Comprehensive coverage of the technical level would require significant documentation that would restate information already maintained by competent technical authority. Included in the integration level will be references to the technical specifics of a particular standard, specification or guidance to allow the reader to obtain greater detail. The integration level addresses each information technology category with an overview that discusses the standards and guidance selected with the associated rationale. A future ITSG document or web page will include a management summary that links the technology summaries for a single source at the management level of abstraction. For this first product, however, the focus of the ITSG is on system integration to improve the operational performance of the information infrastructure.

2.4 System Capability

The four core system capabilities listed below provide the foundation for functional (e.g., logistics, administration, C4ISR, operations) applications. A system architecture, technical standards and guidance will support the development and sustainment of these capabilities across the Naval enterprise. Each of these capabilities is created by a collection of platform/activity systems interconnected and integrated, thereby providing a full enterprise capability. Each system

is determined by considering the platform or activity mission and operating environment. The four core system capabilities are:

Local Area Network (LAN) and Core Client Services. This includes a backbone, hubs and tail segments to devices. The devices include, at a minimum: primary and secondary domain control servers and PC clients for command identified users. Core client services include those required by commands to effect business and operational process improvement across the Naval enterprise.

Dispersed Communication for Deployed Forces. Ships and deployed Marine Corps elements require robust reliable communications into the Defense Information Systems Network (DISN) normally via Satellite Communications (SATCOM) for C4ISR and Tactical Support.

Wide Area Communications for Shore and Garrison Forces. Shore commands and Marine Corps garrisons need connectivity to the DISN to reach deployed forces and other supporting units.

Basic Network and Information Distribution Services (BNIDS). These are the very basic network services and the most fundamental applications that all platforms and activities need independent of their command mission and operating environment. BNIDS include network packet or circuit delivery, domain name service, directory service, electronic mail (e-mail), web service, file storage and transfer, network time service and network news service. (Chapter 6, Information Distribution, contains the full list of BNIDS.)

2.5 Standards, Architectures and Infrastructure

Standards and guidance provide the fundamental elements necessary to allow the components of the architecture to be interoperable. Certification that an infrastructure is built to standards provides the credibility and trust needed by users for safe and reliable operation. Information technology standards and guidance within the Department of the Navy are needed to achieve secure, credible, and comprehensive support of operations and business practices. The metaphor used in the JTA describes standards as the “building code”. Unlike a building infrastructure, which is totally grounded in physical principles, the information infrastructure must become the established discipline and order in a logical environment as well. To build this infrastructure, architecture is needed that supports both the logical and physical environment. Additionally, the architecture needs to be responsive to information technology advancements to ensure infrastructure evolution with attendant improvement in operational practices, ease of use, and minimal disruption.

2.5.1 Supporting Infrastructure Evolution

2.5.1.1 Transitioning the Naval Information Infrastructure

The advancement of network communication technology offers opportunities for greater efficiencies and economies of scale by combining electronic information flow onto a single logical network service. In the past, transport of information on specific physical media drove the technology and associated system management structure. Typically, a separate support and management structure was required for telephone, computer and television/video

teleconferencing systems. We now have the capability to combine voice, video and data transmission onto the same communication network. Figure 2-2 illustrates.

As shown in Figure 2-2, voice, video and data applications currently require separate infrastructures for each information type. Better efficiency, economy of scale, and interoperability are attained by combining all information onto a single integrated network. Edge devices can be provisioned to interface two specific media types.

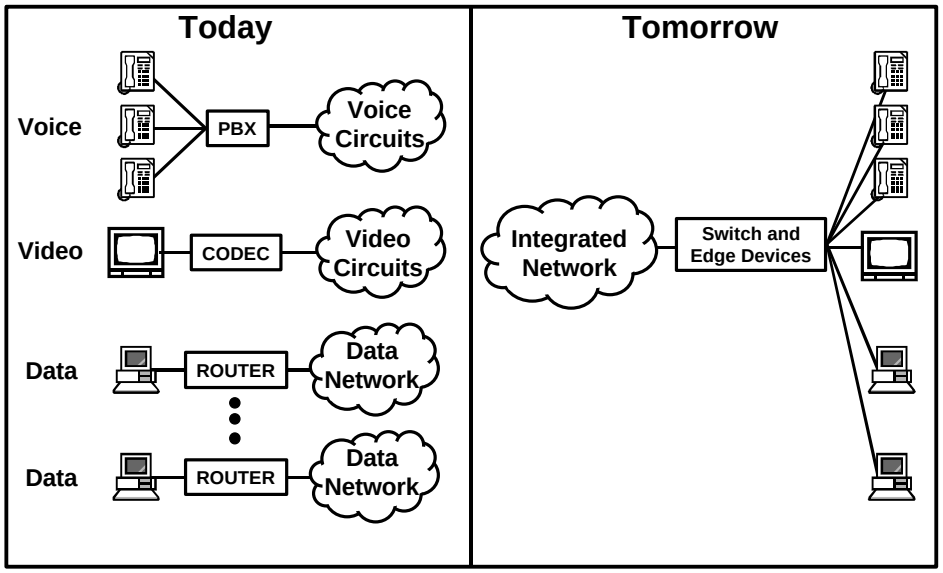

Figure 2-2. Transition of Information Technology

2.5.1.1.1 Factors Affecting Transition

These factors support the consolidation of the information infrastructure:

Economics. The ability to attain better information processing and dissemination capability. The potential for improved economics provides impetus for consolidation of information onto a single infrastructure.

Interoperability. Previously, information transfer and storage decisions were determined based on the physical media used for transport. The ability to mix and match information from video, voice, print and computing was not possible because the protocols and the physical transport media were not interoperable. Digital electronics, advances in protocols, and the technology to support a wide range of transfer rates has removed that limitation. Now, we can combine voice, video, and data on common information systems for improved system interoperability.

These factors support the separation of the information infrastructure:

Security. Until recently, incompatible physical media provided natural separation barriers that mapped to natural security boundaries. As we transition to common protocols and media, new technology and organizational discipline must provide secure separation of information.

Organization and Management. Similar to security, physical media incompatibilities provided a natural scope to the span of control managed by the information system manager. Systems were created based on the media types and entire management support structures were created to manage end-to-end information flow within the media limitation. These system management structures, however, often impede new efficiencies available using common media. Organization and management influences maintain some division of information span of control, but not necessarily those implemented by legacy system management structures.

Economics and interoperability are the basis for consolidation of information technology assets. On the other hand, security and management are the basis for maintaining the separation of these assets. The drivers for these are often in direct conflict with one another, e.g., consolidation may provide economies but can negatively impact responsiveness to diverse customer requirements or integrity of security enclaves. The ITSG seeks to achieve a balance between consolidation of multiple technologies and separation of information technology functions by optimizing all relevant drivers.

2.5.2 Characterizing Information Technology

2.5.2.1 Redefining the Infrastructure

Information technology now offers the capability to provide a single ubiquitous network supporting all information including voice, video and data. To exploit this capability, the DON ITSG IPT has identified the following top-level categories of the Information Infrastructure:

System. The information and data processing resources, associated peripheral devices, supported applications, and the communications network infrastructure that interconnects the end users and components of the system. Systems include hosts, operating systems, peripherals and system applications, databases, and files. A system also includes all hardware and software components, facilities, personnel, and procedures that are necessary to support applications.

Network. The set of switching and transmission subsystem communication components to support information transfer. The network includes all hardware and software communication components residing in switching, routing, and transmission subsystem components, as well as communication-related hardware and software and those components that reside in hosts (e.g., communication protocols). The network also includes the organization and configuration of embedded hardware and software to support orderly and logical information distribution.

Application. A collection of system components that supports a particular task or function. It includes end-to-end, multi-media communications as well as information management and decision support capability. Distributed computing applications are normally built using a three-tiered architecture consisting of the application server, data server, and presentation clients which may be physically on a single device or on multiple devices connected by a network. Communication applications normally involve a minimum of two communication devices connected by the network.

Appliance. Any device by which an end user receives, processes, or transmits information on the selected media. Information appliances include computers, telephones, televisions, video teleconferencing equipment and the like. It is also the hardware component that is part

of an information appliance suite such as a mouse, keyboard, or video screen. In the three-tiered application architecture, these devices are referred to as “presentation clients”.

Information. The assembly and presentation of data in a form that is understandable and valuable for conveying knowledge and making decisions. It is the “payload” of the information infrastructure.

The network forms the foundation for the system, applications and appliances. Appliances are the user’s interface which connect to the network so that data and applications can be accessed. Applications are the software programs, information tools, and databases that the user operates to perform tasks. Applications transcend the network and the appliances. They involve multiple distributed computers and databases including the data server, application server and presentation client software. Application management includes coordination of the network managers and appliance managers so that the program software can access the data and processors needed.

Figure 2-3 and Figure 2-4 respectively provide illustrations of the operator’s perspective and the system manager’s perspective of these system infrastructure categories.

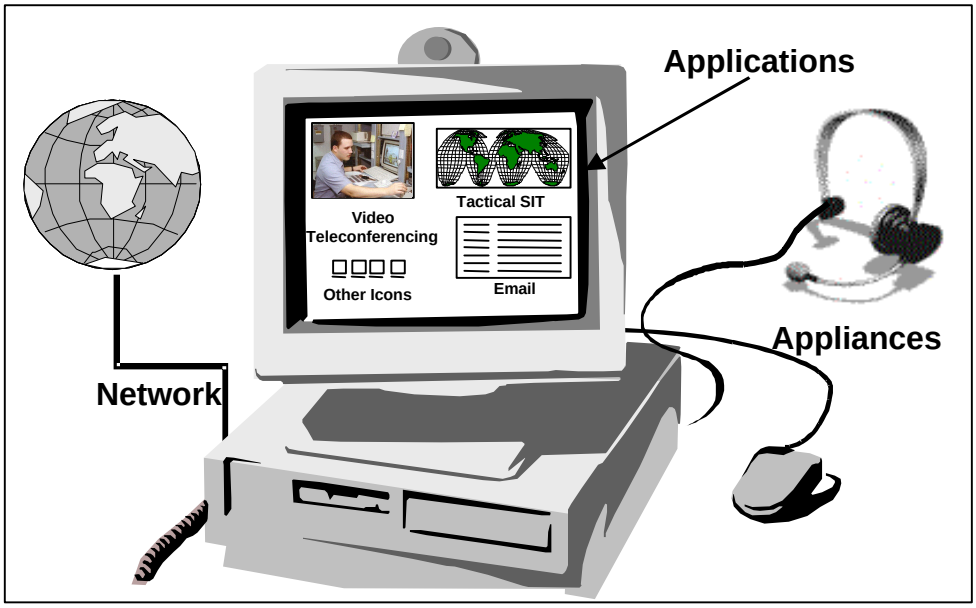

Figure 2-3. Operator’s Perspective of the Information Infrastructure

The operator interfaces with the computer, video equipment, headset or telephone and cares about running applications, getting and transmitting information independent of the physical location of the information.

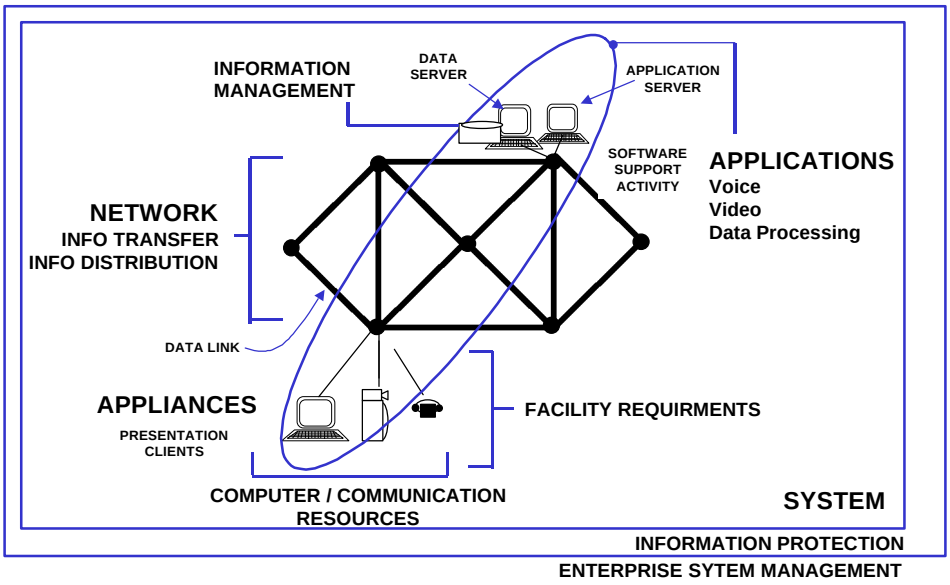

Figure 2-4.System Manager's Perspective of the Information Infrastructure

The system manager cares about appliances, network nodes, links and associated equipment. He also cares about interoperability of the software across the network, with the appliances, various databases and software management facilities that support the end user's application.

2.5.2.2 Information Technology Categories

The simplicity of system, network, appliances, applications, and data is good for the management level of abstraction, however, the system integrator needs greater fidelity. At the system level there are foundation principles that must be considered when implementing any system component. Security and physical requirements (e.g., power) must be met. Additionally, after implementing the system, the entire system must be managed and system quality must be assessed through the use of metrics. Within the network category are components that must be considered in both the physical and logical environments. These can be categorized as "information transfer" for the physical network and "information distribution" for the logical network. The quality and format of the information itself must be considered for use by the applications for processing and presentation. Using the previously defined single ubiquitous network as the model, voice and video systems are considered as applications of the system and are assigned to the applications category. The ITSG provides a level of organized segmentation to the system integrator by arranging and presenting information technology standards and guidance in eight categories. These categories are shown in Figure 2-5 as they relate to the system manager's view (Figure 2-4). The stack shown on the left of Figure 2-5 resembles the seven layer Open Systems Interconnect (OSI) model. The OSI model, however, only applies to internetworking. ITSG information technology categories transcend the network and support total information system implementation to maximize operational capability.

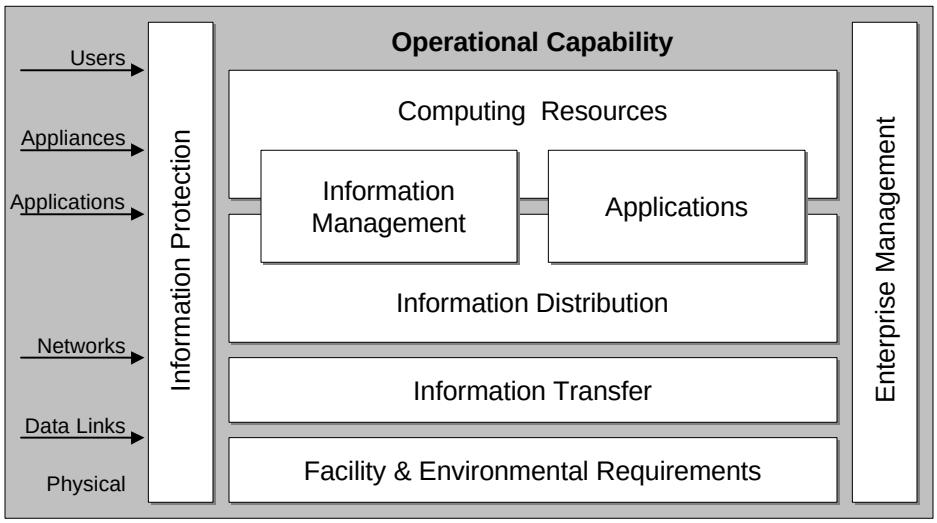

Figure 2-5. ITSG Information Technology Categories

The development of ITSG information technology categories are used to support the transition from an application-based system implementation to an infrastructure-based system implementation. This organization supports convergence to a single ubiquitous network for all applications and information media while continuing to allow for separate networks necessary for security separation and differences in technology maturity.

These categories are intended to organize standards and guidance into groups that focus on each layer of the architecture. Taken together, standards and guidance used from all of these categories will provide comprehensive support of the enterprise infrastructure. The order of the categories is important. In the selection of standards and guidance, certain fundamental security and physical factors have to be established before other standards can be selected. Information Protection is the first category and includes the security standards and guidance that other categories must follow. The Facility and Environmental Requirements category addresses the power, cooling and physical security required for the physical installation. The Information Transfer category addresses communication circuits and the physical, logical link, and network layers of the OSI model to move information across the network. The Information Distribution category addresses the most common protocols and formats needed to process and present information such as e-mail and web service. The Computing Resources category uses the Information Protection, Facility, and Transfer standards and guidance to ensure computers and peripherals are interoperable with the infrastructure and the user through Disk Operating Systems (DOS), Network Operating Systems (NOS) and the Human Computer Interface (HCI). The sixth category, Information Management, addresses the format and structure of data-at-rest so that some commonality of information in data bases and data warehouses exists for presentation, interpretation and use by applications. The seventh category, Applications, addresses the software programs and end-user system capabilities such as voice, video and collaborative tools needed by the operators to perform their mission. The eighth and final category, Enterprise Management, that addresses standards and guidance for managing the information infrastructure and metrics to measure its efficiency and effectiveness across the enterprise. These categories are the basis for each chapter of the ITSG.

2.5.3 The Logical Environment

It is difficult to think and operate in terms of a logical environment. Metaphors are created to link logical concepts with physical realities, hence the use of the term ‘virtual’. For example, the term ‘virtual reality’ labels items that appear to our senses to be actual physical entities but that are actually created through logical configuration and presentation of sensory data. Likewise, the term ‘virtual network’ refers to the logical configuration of what could be multiple physical networks interlinked into a set of networks tailored to a particular operation or business process. This logical environment, with its distributed data, is referred to as “cyberspace” in the Internet culture.

2.5.3.1 Benefits

The logical environment is free of physical constraints and has more degrees of freedom to foster innovation. For example, a worldwide virtual network allows creation of a ‘virtual office’ of individuals widely dispersed over long distances and performing as a single team. In the ITSG, virtual networks and logical networks mean the same thing.

2.5.3.2 Challenges

The multiple degrees of freedom in the logical environment make order and discipline a greater challenge. For example, physical safety is not a direct concern in the logical environment; as a consequence, very little mechanical competence is required to create (or destroy) logical infrastructures. To illustrate, compare the impacts in allowing a four-year old child to drive and crash your car versus allowing him or her to operate and trash your computer’s hard drive – the physical damage is much worse than the logical damage. Conversely, security is a monumental challenge because of the many degrees of freedom available. The ability to traverse many logical environments from a single one is trivial unless logical separation controls are implemented. A constant tension in IM/IT is how to exploit dramatic IT advancements through the logical environment while maintaining the security of critical information. This tension is characterized as security versus freedom. The information infrastructure requires a carefully administered risk management approach that considers a combination of physical and logical measures for adequate security, but enough freedom to be technologically agile and operationally responsive.

2.5.3.3 Virtual Private Networks (VPNs)

With the advent of such technologies as Asynchronous Transfer Mode (ATM), Virtual Private Networking (VPN) has become one of the fastest growing applications of advanced networking technologies. VPNs are logical extensions of physical networking technologies, e.g., physical LANs located in different geographical areas can appear to the user as a single logical LAN – even though a WAN interconnects them. With previous technologies, VPNs were limited because making use of all available bandwidth was paramount to amortize circuit costs. Multiple “bursty” streams were multiplexed via routers to produce a single stream with lower peak demands. This traditional “best effort” scheme was adequate for general data transfer, such as e-mail and file exchange. However, interactive and time/delay sensitive streams had no guarantees that physical networks would deliver information packets on time.

More demanding applications, such as interactive graphics and multimedia, require a more robust approach. A practical solution is ATM. It meets these more stringent demands by offering a more controlled Quality-of-Service (QoS) environment and an accommodation for varying traffic patterns. ATM is a key factor in creating VPNs. QoS will allow network components to multiplex

streams while meeting their latency and bandwidth requirements. With a single protocol that scales from kilobits per second to gigabits per second, and spans LANs and WANs, ATM offers a solution for a global virtual private network – an intranet that rides on shared infrastrucutre.

2.5.3.4 Logical Infrastructure Model

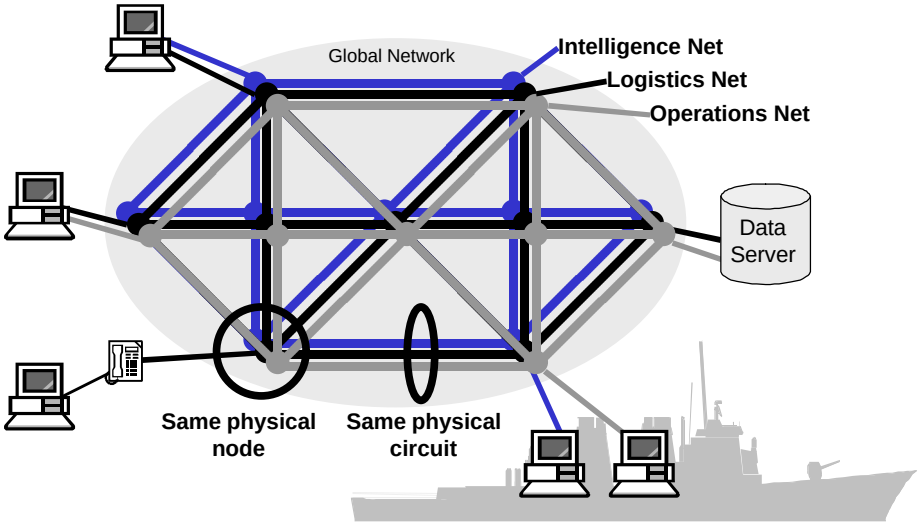

Figure 2-6. Logical Infrastructure Model

Figure 2-6 is a logical infrastructure model that shows three virtual networks supporting five notional users. All users and resources appear to the user to be on the same single network. Physically, other virtual networks share the underlying network links and nodes.

Figure 2-6 provides an example of the simple logical infrastructure model used in the ITSG. As shown, there are three worldwide virtual networks supporting intelligence, logistics and operations, both afloat and ashore, for tactical and tactical-support operations. These networks could represent a network supporting a particular project, releasable information and accessibility to selected foreign nationals, or any other mission area information domain. The underlying physical infrastructure is transparent to the users of the network. All users have access to multiple virtual networks and an information server that supports multiple virtual networks. From a security standpoint, information can flow on common circuits though common, redundant switches and routers. However, at each node, additional protection, encryption and filtering is performed to ensure that only the community of interest can access workstations, processing centers, and information sources. Special measures are taken at the physical network interface nodes to protect against outside or public intrusion.

2.5.4 Area Network Designations

2.5.4.1 Background

As computer networks evolved, different technologies were best suited for the different distances covered. Local Area Networks (LANs) consisted of a network media shared by numerous computers and peripherals under a single management control. Wide Area Networks (WANs) consisted of point-to-point links that connected LANs together using routers, gateways or bridges. Metropolitan Area Networks (MANs) were contrived as small WANs – point-to-point links that connected a relatively high concentration of LANs together within a regional area. LANs, MANs

and WANs were interconnected to maximize computer communication capability among network subscribers. The designation of a particular network as a LAN, MAN, or WAN was primarily due to the domain of circuits and nodes that was under a single management control, normally aligned with the geographic area of coverage.

2.5.4.2 Paradigm Shift

New switching technology combines the best characteristics of shared media and point-to-point network protocols. It can directly connect a multitude of end users over great distances without the traditional network gateways. Hence, the use of "geographic area" to designate a network perimeter is losing its relevance. Because the predominance of this new technology fosters physical and logical networks that transcend geography, the definitions of LANs, MANs, WANs, and related "area networks" have become ambiguous. An "area" no longer bounds the network domain; therefore a new understanding has to be adopted. All of the below descriptions are valid and at least one is relevant, depending upon the point of view of the information worker (see Figure 2-7).

Economic definition: LANs are networks that the user owns, and WANs consist of services that are purchased from an external service provider (either commercial or a corporate department significantly removed from the user). The language of the telephone industry applies – the circuit demarcation point defines the boundary.

Geographical definition: LANs historically spanned a room, ship or building while WANs crossed the country. As LAN technology expanded to network multiple buildings, the terms Metropolitan and Campus Area Networks were created. The advent of high-speed local-loop technology and end-to-end switching, as in ATM, has further blurred this definition.

Control definition: From a network manager's point of view, it is reasonable to treat the control domain as a LAN, and everything outside that domain as a WAN. This definition does not necessarily have geographic significance, but the entry/egress point between the LAN and the uplink network (e.g., the Internet) is the defining boundary.

Other factors that closely relate to the LANs and WANs definition:

Security definition: LANs traditionally stopped at the user side of a router or firewall. With Virtual Private Networks (VPN), geographically separated LANs can now be bridged into a single community of interest.

Bandwidth definition: Until recently, LANs could sustain higher orders of magnitude transfer rates than those of WANs – namely 10's and 100's of Megabits Per Second (Mbps) for LANS versus 1's and 10's of Mbps for WANs (see 5.1.3). The gap in the two rates has rapidly closed as increases in long-haul bandwidth have far outpaced increases in LANs. Because the cost per bps of bandwidth is still significantly higher with WANs, the traditional definition is still valid in many cases. Also associated with bandwidth, bit error rates in WANs can be higher, particularly in shipboard communications.

Standards definition: LANs were standardized in ANSI and IEEE while WAN components were generally standardized by ITU-T (formerly CCITT). The formally designated Metropolitan Area Network (MAN) standard (IEEE 802.6) has not seen widespread use or vendor support. Homogeneous switching fabrics, such as ATM, blur this definition. Because this is a generic definition, it is of marginal use.

The adopted convention could be characterized by the same names but not necessarily the same description. The appropriate definition of a LAN, MAN or a WAN depends on the management, application, and architecture and may change as a system expands. This document provides the standards and protocols necessary to develop various architectures, based on the design goals of the system engineer or system manager.

Characteristics	Local Area Networks (LANs)	Metropolitan Area Networks (MANs)	Wide Area Networks (WANs)	Virtual Private Networks (VPNs)
Geographic	Room, Platform, Ship, Building, Campus	Campus, Base, Town, City, Metropolitan Region. Local Loop Connects To The WAN	Region, Country, Theater, World	Not Applicable
Economic	Implemented by a program of record with appropriated funds or by the command using command budget	Services purchased from a carrier or owned and operated by a DISA or Service regional center	Services purchased from DISA or a commercial carrier	With ATM or single vendor IP routing network services, cost of tailored configuration by command budget or appropriated funds
Control	Single management within the end user command	Single or multiple management outside the end user command	Single or multiple management outside the end user command	Single or multiple management outside the end user command
Security	Safe trusted enclave behind a security firewall and encryption device.	Safe enclave consisting of interconnected enclaves all behind a single security firewall. Classified links are bulk, link or source encrypted.	Some protection of interconnected enclaves each with their own firewall. Links are normally bulk encrypted	Safe trusted enclave based upon source or link encryption of channels and trusted computer hosts and facilities within a community of interest
Bandwidth	Megabits to gigabits per second on a single channel	Kilobits to megabits per second on a single channel. May have channel aggregation.	Kilobits to Megabits per second on a single channel. Megabits to terabits per second on the aggregated trunks.	Megabits to gigabits per second per channel. Aggregate is a WAN
Standards	ANSI, IEEE 802.2 series (Ethernet) TCP/IP, ATM	IEEE 802.6 (little use). ATM, TCP/IP, PPP, ITU-T	ITU-T (CCITT), PPP, TCP/IP, ATM, Frame Relay	TCP/IP using single vendors for routers. ATM

Figure 2-7. Comparison of Area and Virtual Private Networks (VPNs)

2.5.4.2.1 System Manager View

To the system manager a network is simply the domain of circuits and nodes that fall under a single management control. There can be several network domains in a command and/or a single network domain can serve many commands over a very wide area. Geographic distance has little or no relevance to the control domain. In the ITSG, network domains will normally correspond with the Information System Domain (ISD) concept described in Section 2.5.6.

2.5.4.2.2 User View

To the end user, the concept of LANs, MANs and WANs is useful to perpetuate because it aligns the network domain with the physical or geographic domain with which we are familiar. Because of this, the ITSG will continue to refer to LANs, MANs and WANs as they relate to the end user.

2.5.4.3 Adopted Convention

The "area network" conventions adopted by the ITSG are shown in Figure 2-8.

Local Area Network (LAN). LANs use the IEEE 802, ANSI, and ATM standards — the signals travel over optical fiber cable or copper wire and all network components are under the ownership and control of the network manager. They include wireless LANs that are generally designed to support untethered network-to-end-user connections. The control definition applies here. Extended LANs include base and campus networks.

Wide Area Network (WAN). WANs are divided into two parts. The first is defined as trunk technology and switching (Telephony DS-n/T-n and Synchronous Optical Network (SONET) OC-n transport, and ATM and Frame Relay switching). For this part, the economic definition applies – the LAN provider will generally purchase these services rather than invest in wide-area equipment and cable. The second addresses what the telephone industry refers to as the "local loop," meaning the reach from the central office to the business or residence. In many cases, the customer may actually own such assets. (See Table 5-1 for a listing of DS, T and OC link designations.)

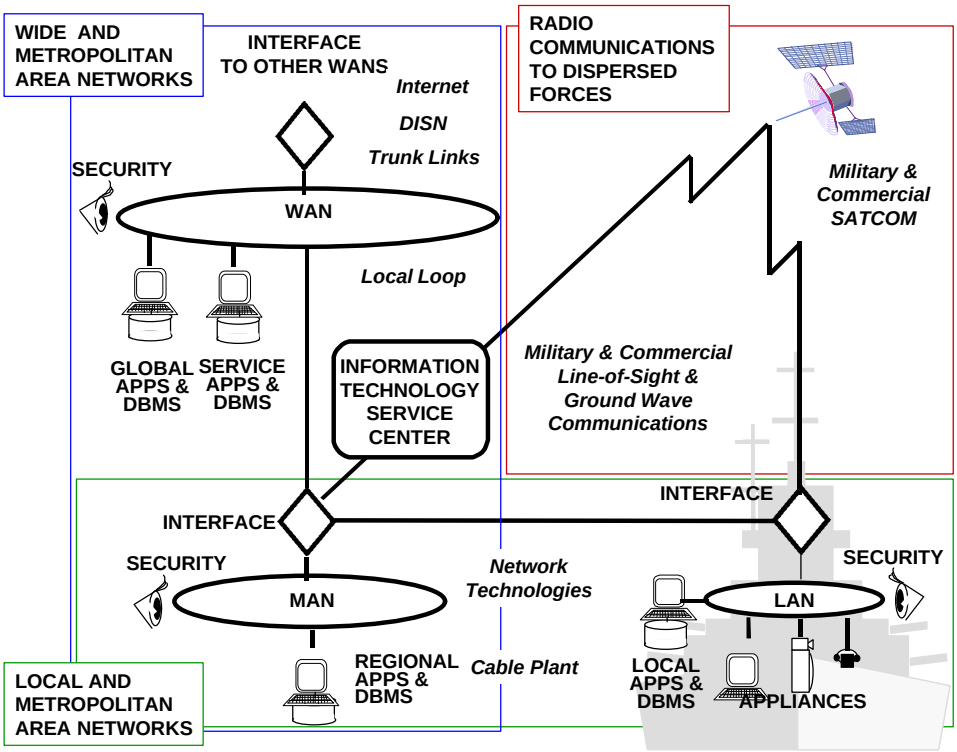

Figure 2-8. Adopted Architecture Model for LANs, MANs, WANs, and Radio Communication to Dispersed Forces

Metropolitan Area Network (MAN). MANs cover the ambiguous overlap where relatively wide area networks can take on the characteristics of a LAN or a WAN. MANs either use LAN technology extended over a "larger" regional area or use WAN technology – point-to-point links that connect a relatively high concentration of LANs together – within a "smaller" regional area.

Radio Communications to Dispersed Forces include Satellite Communications (SATCOM) and Line-of-Site (LOS) radio links to support trunk (router-to-router or switch-to-switch) connections to underway or deployed forces.

2.5.5 The Physical Environment

Figure 2-9 is an architecture model of the global infrastructure showing worldwide coverage and command echelon support from major command headquarters and global information service providers down to the tactical elements. As discussed in Section 10.5.4, the use of WANs, MANs and LANs here depicts network domains that conveniently align with geographic areas and command echelon. This is useful to illustrate multiple networks with required interfaces even though new switching technology can directly connect end users on very large networks over great distances without traditional network gateways. The model shows separate WANs, use of a worldwide fleet intranet for mobile ships, regional and base MANs for garrison and shore commands regions, LANs within the commands, and connectivity to mobile users and tactical units.

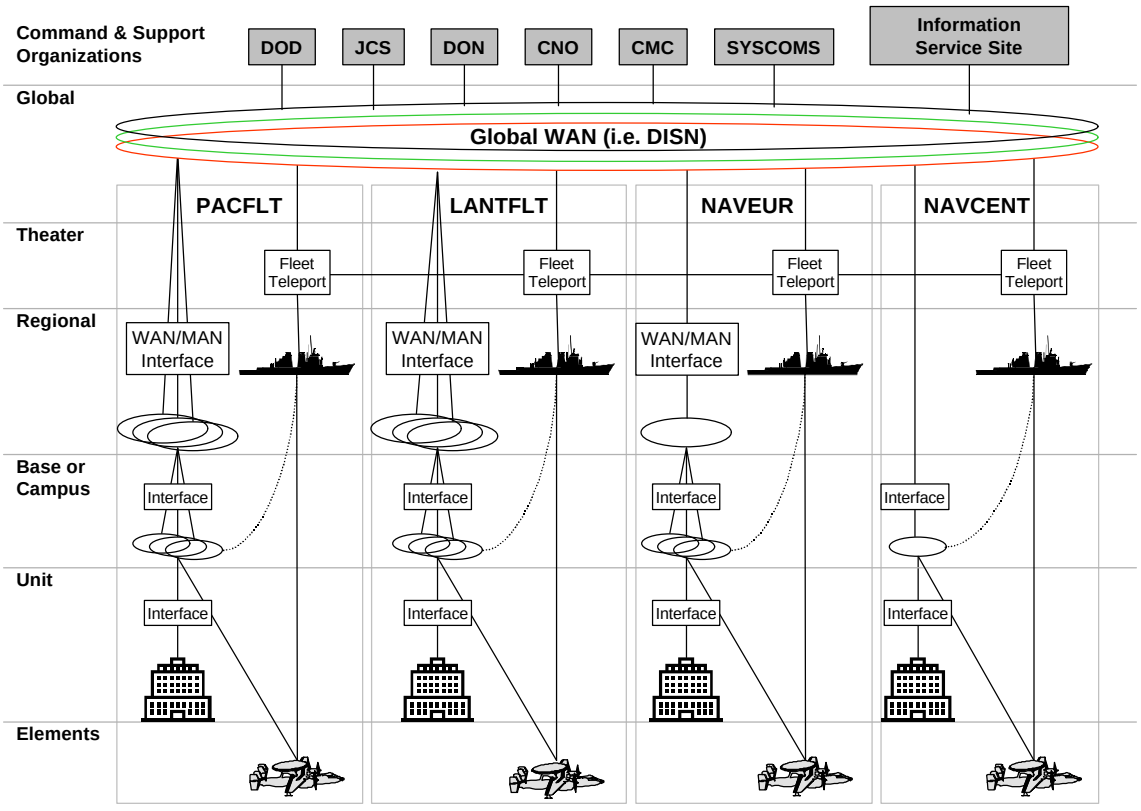

Figure 2-9. Global Infrastructure Model

Section 2.5.3 discussed the logical environment as the needed end-state to be supported by the physical infrastructure. The physical infrastructure model that supports the enterprise (represented

in Figure 2-9) shows both the geographic coverage and coverage of command echelon. Command echelon coverage is roughly the same as geographic coverage but the lower levels of the echelon focus on support of specific missions or functions. A WAN such as the Defense Information Systems Network (DISN) provides global geographic coverage. Security separation is provided by cryptographically-separated networks for Unclassified, Secret, Special Compartmented Information (SCI) as well as the Internet. Currently, the DISN is a single physical network logically separated into the Secret Internet Protocol Routing Network (SIPRNET) and the Non-Classified Internet Protocol Routing Network (NIPRNET). Units can connect directly to the global WAN but in Naval concentration areas such as Norfolk or San Diego, the global WAN / DISN is accessed via a MAN. Deployed units such as underway ships connect to the global WAN via Fleet teleports at each Commander-in-Chief (CINC) site (e.g., CINCPACFLT) and at the Commander, U.S. Naval Forces, Central (USNAVCENT). Ships are provided with seamless connectivity as they move between satellite footprints and from port to port via a Fleet intranet. This links each fleet interface to permit coordination and reconfiguration as necessary ashore to minimize configuration changes performed aboard ship and tactically deployed units. At the Naval concentration areas, shore and garrison commands are connected to base area networks. The base area networks also have connectivity to the Fleet intranet at the piers so that ships can transfer connectivity from their Satellite Communication (SATCOM) systems to pier connectivity, and vice versa, with minimum disruption of information flow. Tactical units assigned to afloat or shore commands will have communication tethers either to their parent commands or to standard network interfaces. Mobile commands or individuals on the road are also able to connect via the standard network interfaces. Information Technology Service Centers (ITSCs) will provide support to Naval components. These centers will function as a single, integrated entity.

2.5.6 Information System Domains

To achieve full integration, the architecture model is further defined to identify zones of the global infrastructure that can operate with relative independence from the remainder of the architecture. Normally, the zones are the area networks such as the LANs, MANs and WANs and the routers or gateways are the interface. These zones are designated as “Information System Domains,” (ISDs) (Figure 2-10) which include a set of clients, servers, multi-media equipment, associated peripherals and network components interconnected and bounded by interfaces to external networks or communication circuits. The ISD is managed and operated by a single organization. The information system domain concept provides the freedom to allow changes in zones of the infrastructure with minimum impact on the enterprise. The following provides additional advantages of the information system domain approach.

- Recognizes that different platforms have different operational missions and must operate in different environments (e.g., latency requirements for targeting data on a Cruiser versus delivery of orders for a Personnel Support Detachment (PSD)).
- Tolerates a “system flux” across the entire infrastructure. Allows for technology refreshment with less coordination. Different versions can be allowed as long as contained within the ISD
- Allows for some command autonomy
- Allows for a modular approach to standards implementation
- Allows exploiting new technology in controlled domains

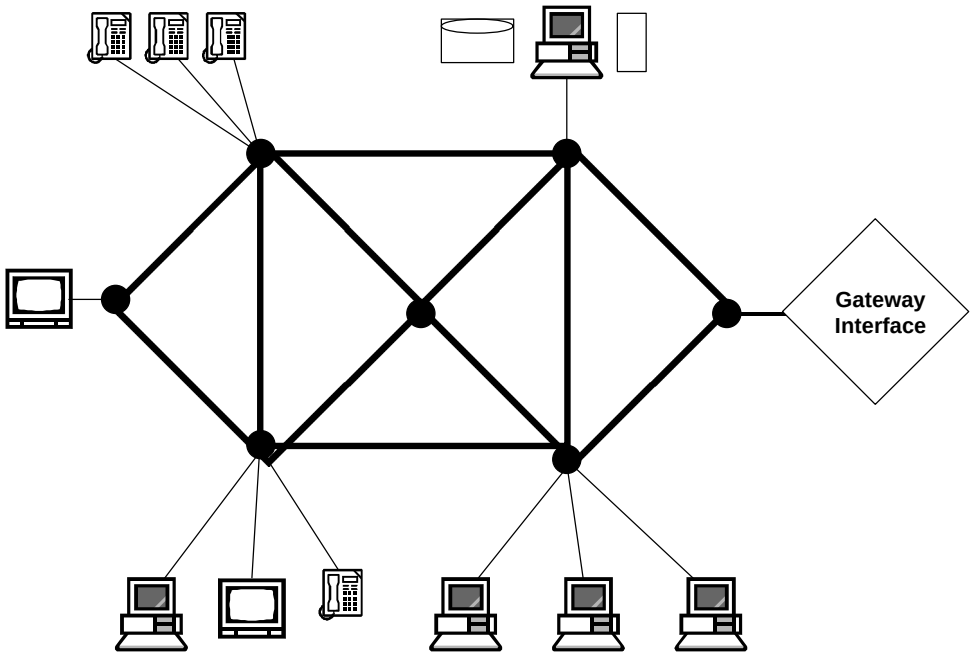

Figure 2-10. Information System Domain

2.5.7 System Domain Components and Linkages

Information system domains provide tolerance for information technology differences caused by budget and operational constraints. Critical to the establishment and sustainment of a single enterprise-wide system infrastructure is control of the interfaces between the Information System Domains. Normally, the information system domains will be a geographic area network such as a local, metropolitan, or wide area network. Each domain will have a number of interfaces consisting of devices such as routers, switches, firewalls, proxy servers, and encryption devices. These interfaces must use common standards and be strictly configured to achieve enterprise system component interoperability and integration. Figure 2-10 is a lower level view of the architecture model depicted in Figure 2-9. Figure 2-11 shows each area network from the command's LAN through the regional MAN (which can also represent the Fleet intranet). The MAN is shown connected to a WAN via an interface that in turn is connected to another WAN via an interface. Many Information System Domains will have information and application servers that can support the entire enterprise or the local region and all have to implement consistent security measures to protect the enterprise. Selection of standards and guidance is based upon using Figure 2-11 to support enterprise integration and the logical infrastructure model depicted in Figure 2-6 to support functional area networks that transcend geographic locations.

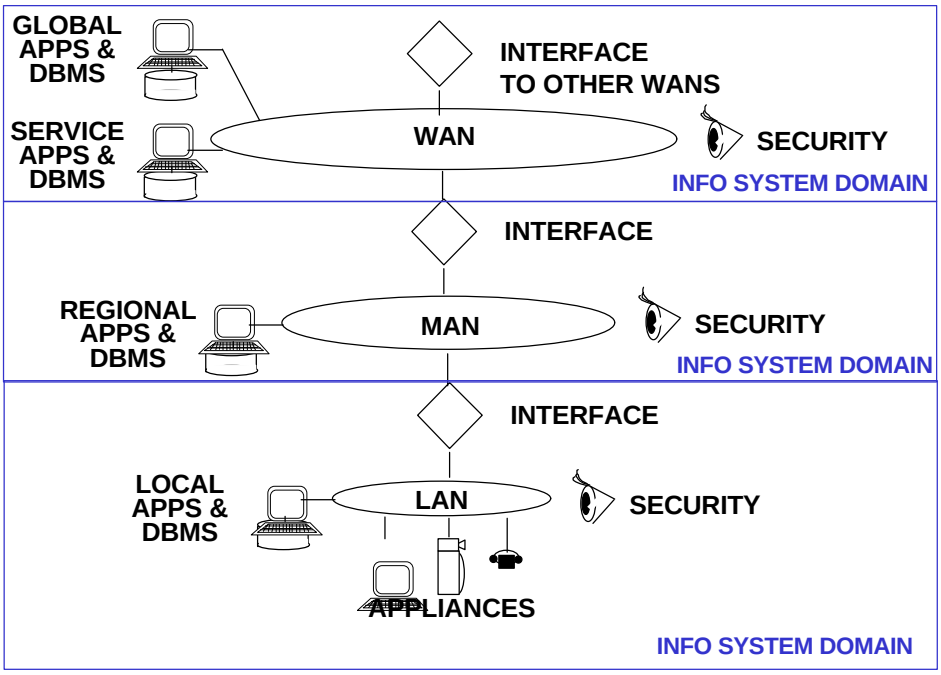

Figure 2-11. System Domain Components and Linkages

2.6 Platforms, Activities and Operating Environments

Discussed in Section 2.4 were the core capabilities that individual systems, implemented on a combination of platforms and activities, could provide for the enterprise. In the Naval environment, it is unrealistic to expect all platforms and activities to use a "one size fits all" set of standards. The specific selection of standards depends upon the platform or activity being considered. The intensity of the command mission and the characteristics of the operating environment drive the specifications called for to implement information systems. Consider the mission and operating environment of an aircraft carrier versus a Personnel Support Detachment – the command mission and operating environments are vastly different and require separate standards profiles, particularly for the external interface. To provide standards profiles that support required information flow across the Naval enterprise, categories of platforms and activities are defined. These platform/activity categories and subcategories tailor standards and guidance to meet the command mission within the operating environment of each platform.

Ships. The ITSG provides guidance specific to shipboard tactical and non-tactical systems and supporting communications. The unique performance requirements (e.g., survivability, vulnerability, latency, etc.) were judged to require specific focus on the standards and guidance relevant to nine sub-categories of ships. The nine include:

- Command Ships (LCC, AGF)
- Carriers (CVN, CV)
- Missile Shooters (CG, DDG, FFG)
- Submarines (SSN, SSBN)

- Other Combatants (DD, FF, PC)
- Large Amphibs (LHA, LHD)
- Small Amphibs (LPD, LSD, LST)
- Logistics (AO, AOE, AS, AG, AE, ARS)
- Auxiliaries(AGSS, MCM, MCS. MHC)

Information Technology Service Centers (ITSCs). The ITSC is proposed as a nexus of engineers, technicians, and administrators that use system management tools to provide comprehensive IM/IT support to the Naval information infrastructure. The ITSC provides information system operation, implementation support, and administration for a community of information producers and consumers. The ITSCs should be "Local Control Centers" in full compliance with the Joint DII Control Centers Concept of Operations (CONOPS). Each ITSC would perform three major duties:

- Provide integrated information system implementation, control and maintenance
- Interface information flow from network to network including dial-in service
- Provide consolidated information and application servers, and serve as the distribution center for individual commands in the region

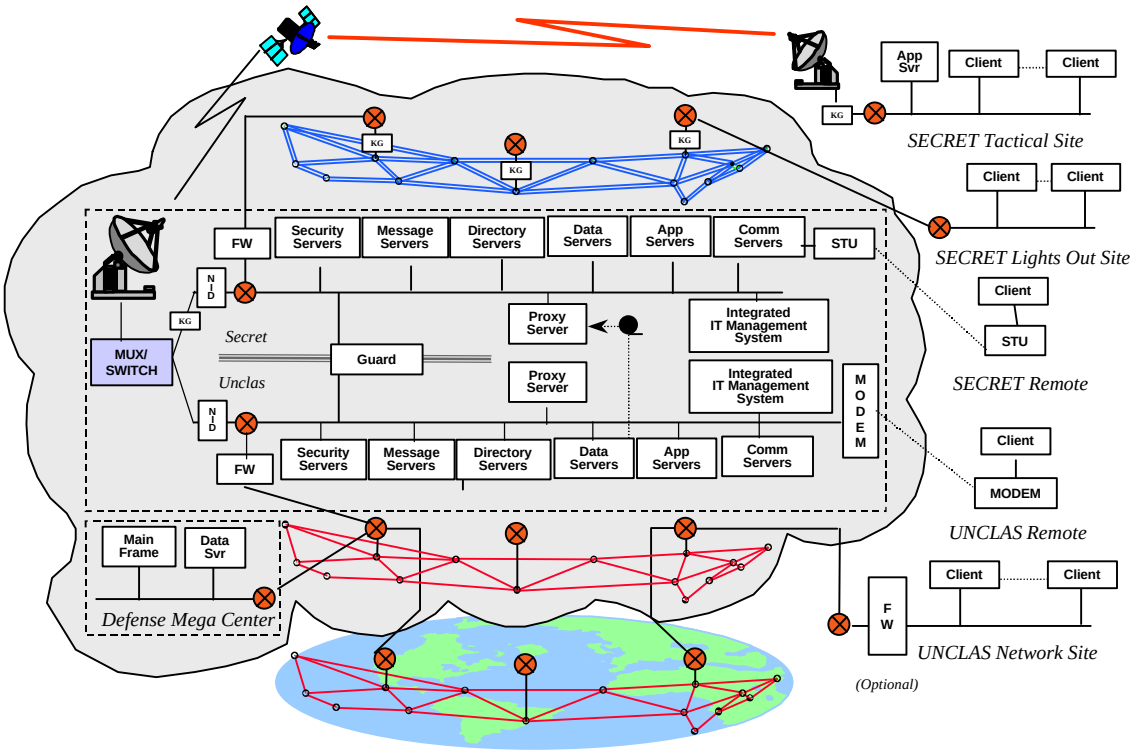

Figure 2-12. Information Technology Service Center

In Figure 2-12, the contents of an ITSC is shown within the dashed box including information servers, application servers and an integrated IT management system. ITSCs are

distinguished from shore commands by their critical infrastructure support and interface. They also provide a "pivot" to minimize disruption in service for ships that come into port and staffs that embark. ITSCs are discussed in more detail in Chapter 10.

Garrison/Shore Commands. The shore-based garrisons and commands have a wide range of tactical and non-tactical operations and support requirements. Peculiar requirements specific to location, mission, media, and other criteria require that the following sub-categories of these environments can be specifically addressed.

- CINC Joint
- CINC Fleet
- CDR Type
- CDR Force
- CDR Region
- CDR Group/Squadron
- Base-Station
- Air Wing/Squadron
- Group-Squadron
- Marine Garrison
- Medical/Dental Facility
- Training Facility
- Maintenance Facilities - Air Rework Facilities and Shipyards
- Technical Support – Laboratories, System Centers and Engineering Centers
- Personnel Support Activity (PSA)- Personnel Support Detachment (PSD)
- Small Craft Support
- Construction Battalion (CB) Facility
- Explosive Ordinance Disposal (EOD) Facility
- Supply Facilities - Depots and Weapon Stations
- Miscellaneous Facility - Naval presence at Contractor sites

Embarkables. This operational environment considers a command that must routinely move between shipboard and shore environments. The emphases for embarkables shall be on portability and "snap-in" connectivity in the corresponding ship, shore, air, ground and ITSC environments. The following types of commands can be considered embarkable.

- CDR Numbered Fleet
- CDR Group/Squadron
- Air Wing/Squadron
- Embarked Support Staff
- Embarked Marine Expeditionary Unit (MEU)

Ground. This combat-focused environment has very unique and demanding information technology requirements. This category will primarily focus on the Marine Corps and mobile command centers such as a Mobile Ashore Support Terminal (MAST).

Air. This includes the system components in the airborne communications operating environment. This will expand over time to include connectivity across different airborne platforms.

Space. This is an emerging operational environment that must have standards specific to this mission. This category will evolve over time.

To assemble a profile of standards and guidance that will provide the four core capabilities (Section 2.4) across the Naval enterprise, all information technologies must be applied against each platform and activity mission and operating environment. Figure 2-13 provides a matrix that depicts the specific information technologies that are appropriate to the particular operating environments. This matrix provides a framework for profiles of standards and guidance in each information technology category (the column of the matrix) with a focus on enterprise integration. With all the columns complete, a row would represent a guidance profile that addresses the operating environment and mission of a specific platform or activity. In the initial ITSG, the focus is on technology-based profiles for the enterprise. Subsequent updates to the ITSG will evolve to accommodate both technology-based and activity/platform-based standards profiles.

OPERATING ENVIRONMENT & PLATFORM CATEGORY	INFORMATION TECHNOLOGY CATEGORIES: Information Protection	Facility & Envir. Requirements	Information Transfer	Information Distribution	Computing Resources	Information Management	Applications	Enterprise System Mgt
Shipboard Environment Command Ships Carriers Missile Shooters Submarines Other Combatants Large Amphibs Small Amphibs Auxiliaries Logistics								
Info Technology Service Centers								
Shore Environment CINCs & CDRs Base-Station Group-Squadron Marine Garrison Air Wing/Squad Medical/Dental Facility Training Facility Maintenance Facility Tech Support - Lab PSA-PSD Small Craft Support CB Facility EOD Facility Supply Facility Misc Facility								
Embarkable Environment								
Ground Environment								
Air Environment								
Space Environment								

Figure 2-13. Operating Environment Matrix

2.7 Currency of Standards and Guidance

Rapid evolutionary advances in information technology are expected to continue unabated – with resultant continued short technology life spans. These life cycle patterns can be represented and explained by “S” curves. Associated with the “S” curve is the “cost trough” that reflects an area of lowest cost as impacted by competition and availability of the technology. The “S” curve enters this trough when the technology usefulness and acceptance emerge and benefits begin to rise. The cost trough continues until saturation or maximum capability is reached and remains until rendered less beneficial by emerging/new technology. Likewise, the cost curve starts to rise as more support and alterations are required to interface the aging technology with new

technology. “S” curves can also be used to track and anticipate innovation cycles. Overlapping “S” curves within a technology domain often show where the benefits of one innovation peak and decline, while the next innovation gains acceptance and accelerates. By comparing specific technologies with other important technologies in the industry, organizations can better anticipate and plan.

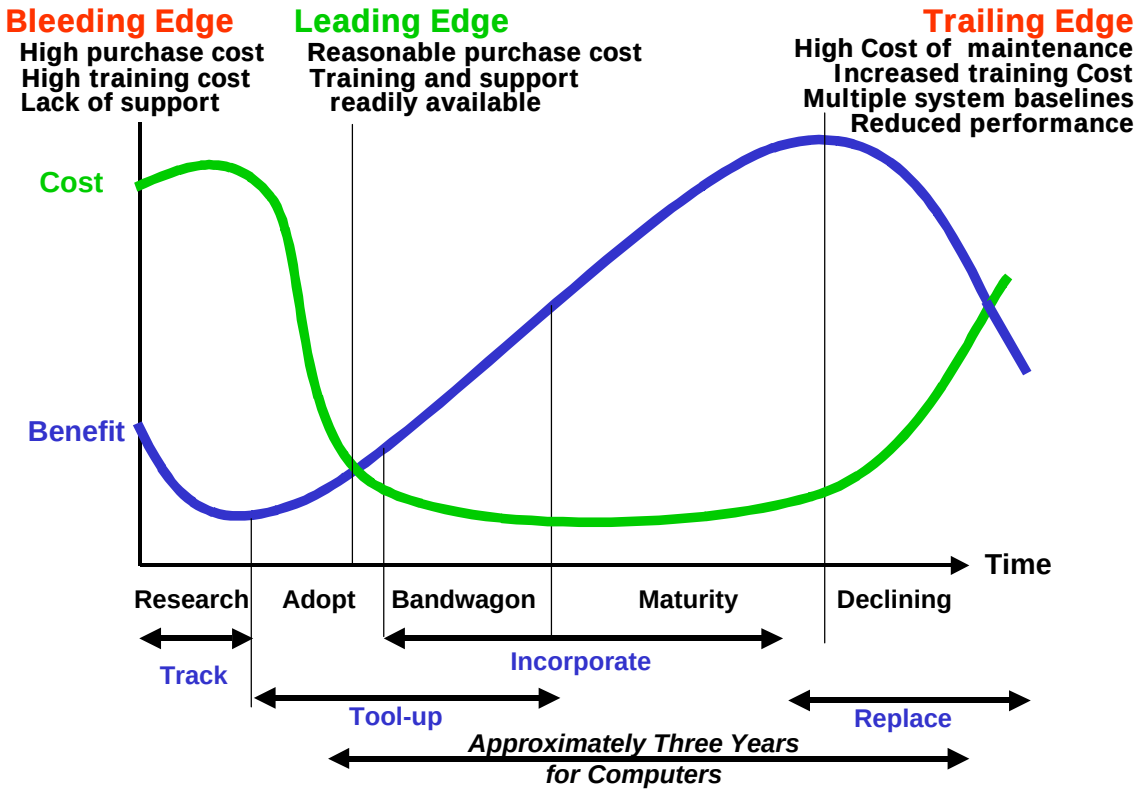

Figure 2-14. Technology Life Span

Shown in Figure 2-14 is the benefit “S” curve that starts low but peaks as the technology matures. Likewise the “cost trough” goes from high at the “bleeding edge” of the technology, bottoms as the technology matures, then increases as the technology becomes less popular and is more difficult to support. The pace of IT innovations has increasingly shortened the life spans of IT products. The technical complexity of products is also increasing. The high mobility of forces and rotation of support personnel make this product turnover and complexity especially acute for the Navy and Marine Corps. Figure 2-15 depicts a recommended ITSG implementation structure for a specific technology life span. This table will be used throughout the ITSG to provide guidance to commands to plan and budget for required infrastructure changes. DON IM/IT strategy will change at a reasonable rate – one that keeps us current but minimizes changeover disruption. Use of the Information System Domain concept (in Section 2.5.6) will allow for incremental change across the Naval enterprise while maintaining enterprise-wide interoperability.

<table>
<tr><td></td><td>Current ITSG</td><td colspan="3">Projected ITSG</td><td></td></tr>
<tr><td>Not Recommended</td><td>1999</td><td>2000</td><td>2001/2002</td><td>2003/2004</td><td>Emerging</td></tr>
<tr><td>Selecting any of these specifications, products, or technologies is not recommended.</td><td colspan="4">Select specifications, products, or technologies based on this time line.</td><td>These specifications, products, or technologies are being monitored as potentially significant.</td></tr>
<tr><td colspan="2">Activities, Platforms, Operational Environments</td><td colspan="4">The specifications, products or technologies above apply to these platforms or operational environments.</td></tr>
</table>

Figure 2-15. Sample ITSG Implementation Time Line

- The Not Recommended column specifically identifies certain technologies, specifications or products that significantly deviate from the preferred direction due to lack of interoperability, security, supportability, etc. The information system implementer should avoid selecting technologies or products listed in this column.
- The dated columns provide a time reference for choosing and aligning with DON technology direction. The standards and products listed in these columns constitute the guidance for the years depicted.
- The Emerging column highlights specifications or guidance that are potentially significant but are not convincing enough to appear on the time line of current ITSG. DON activities are monitoring these specifications and guidance for development maturity.
- The order in which entries are listed within a column has no significance.

2.8 Degree of Compliance

The last element in the ITSG approach is the degree of compliance required. There are clear advantages to making all elements of the ITSG mandatory. However, the dynamic nature of information technology, its different applicability to each operating environment and mission, and necessity to rapidly integrate emerging technology dictate the need for some latitude in compliance. To give the IT system implementer or manager comprehensive guidance on the strength of the need for compliance, three degrees of compliance will be associated with each ITSG:

Mandatory. These items must be followed under the conditions indicated without deviation. This original release of the ITSG contains no mandatory guidance.

Recommended. These items should be followed under the conditions indicated but deviation is allowed to account for special circumstances determined by on-site system managers or system developers.

Proposed. There is no requirement to follow this item. It is provided to allow advance planning. This would be associated with an emerging specification or guidance.

2.9 Standards and Guidance Selection Criteria

The DON CIO has established a standards selection criteria to be used in developing the DON IT Standards Guidance. The specific guidance given in selecting standards is that they should meet

the following criteria: (1) security, (2) functionality, (3) interoperability, (4) performance, and (5) business issues.

Security. Information protection involves both system security and information security. Selected standards must support the ability to provide both system and information security.

Functionality. Standards and guidance must support the fundamental requirement to ensure that IM/IT systems effectively and efficiently support the operational mission/requirements.

Interoperability. Applications and computers from different suppliers will have the capability to work together on a network and to connect and share data and processes as appropriate. The model that the standards in this document follow is one that allows end systems to attach to any point on an internetwork. (End systems include clients, servers, and sensors that produce or utilize information.)

Performance. The degree of quality that a particular standard or guidance provides in selecting IM/IT products or services.

Business. Implementation cost and market acceptance of the standard or guidance is also a selection factor. Market acceptance is judged more on market momentum than on current market share. A dominant product may actually be losing market share, while an emerging product or standard may be rapidly increasing its share. By including market acceptance as one of the selection criteria, we obtain a balance in theoretical versus practical value as based on the market conclusions regarding technology, functionality and value.

2.10 Enterprise Standards and Guidance Profiles

The standards profiles specify the standards and implementation approaches to build the systems across the entire IT spectrum, for a DON platform, activity or across the entire enterprise. These profiles include standards and guidance that address critical hardware, software, communications, data management, security, and user interface characteristics. Profiles support interoperability across platforms and applications.

2.10.1 Profiles

A profile is a set of specifications bundled together to describe the technical standard for a function or a service (such as operating systems, network, and data interchange services), and will include minimum criteria for the information and technology that support specific functional requirements. Profiles equate to the lowest level business process, and document agreed-to implementation requirements used in building and operating systems. Systems using the same standards, but different options, will probably not interface correctly. For example, e-mail services would be defined in the DoD Technical Reference Model and would have an associated standards profile that defined required features for e-mail within the agency.

2.10.2 DOD Technical Reference Model

Of particular importance is the DOD Technical Reference Model (TRM) for assembling profiles across the following technology categories:

- Computing Resources

- Information Management
- Applications

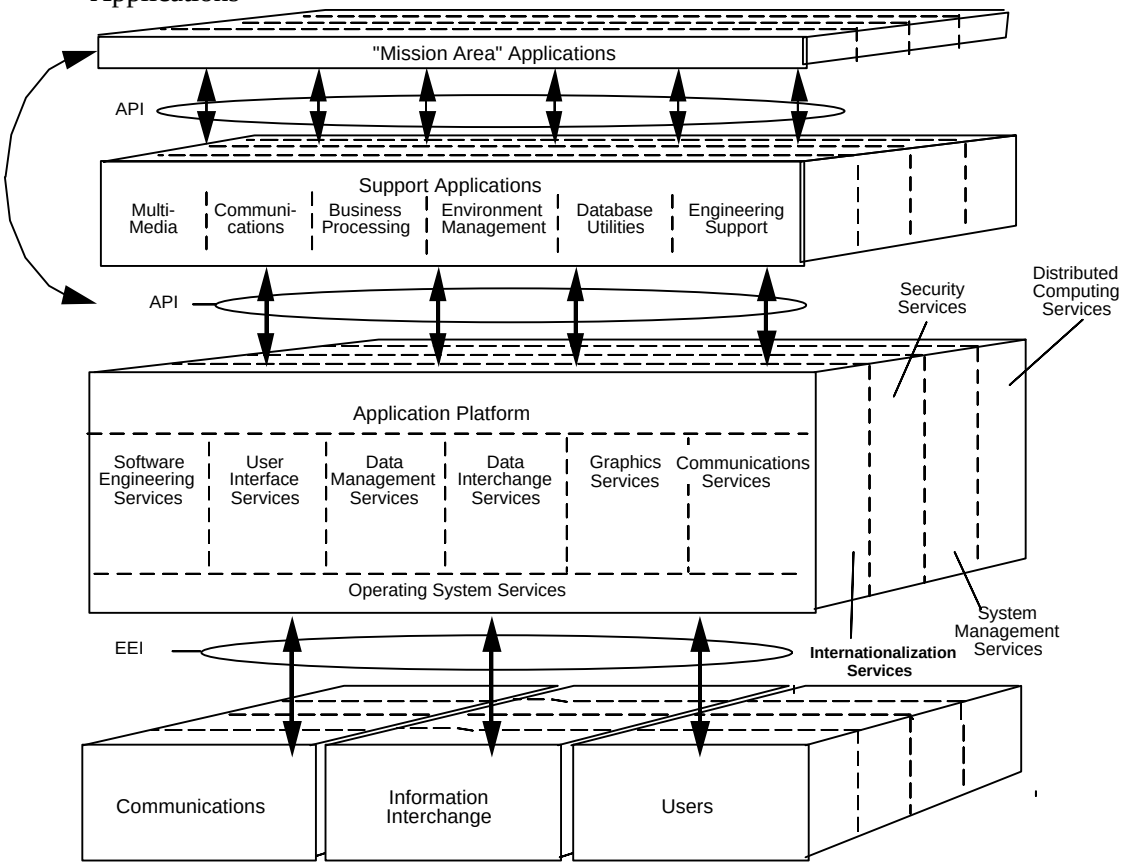

Figure 2-16. DoD Technical Reference Model (Version 3.0)

The DoD TRM shown in Figure 2-16 provides a conceptual framework and common vocabulary of services needed in each of the standards elements. The TRM identifies and specifies the support services (multimedia, communications, etc.) and interfaces that provide a common operating environment and support the flow of information among enterprise and common support applications. This model represents the computer resources, information management and applications categories and interfaces with the communication and networking technology categories that are appropriately represented by the ISO Open System Interconnect model. The DoD TRM addresses standard profiles that provide seamless application support over widely distributed computing resources and attendant interfaces between the computing resources and other technologies. It is important to note that this DoD TRM is platform-centric and cannot be used as the sole framework for a network-centric environment.

2.11 Promulgation of IT Standards and Guidance

Figure 2-17 illustrates how each chapter is organized. As shown, there will be an overview that provides a summary of what is contained in the chapter. Some chapters will also have a background section to provide a foundation to understand the contents. Within the body of the chapter, topics will be introduced and discussed. An associated statement on the implementation of the standard, specification or guidance will be followed by a table showing the recommended implementation over time for different platforms. Each chapter will close with a list of references.

The official references of the standards and guidance will be provided as well as any sources supporting the chapter.

Overview

Background

Topic

Description

Discussion

Best Practices

Recommended Implementation

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
Avoid selecting any of these specifications, products, or technologies	Select specifications, products, or technologies based on this time line.				These specifications, products, or technologies are being monitored as potentially significant.
Activities, Platforms, Operational Environments	The specifications, products or technologies above apply to these platforms or operational environments.				

Notes

References

Sources for Standards Guidance

Supporting Resources

Figure 2-17. Generic ITSG Chapter Outline

2.12 References

Joint Staff, J6, “C4I For the Warrior” 12 June 1992

Joint Staff, “Joint Vision 2010, America's Military: Preparing for Tomorrow”; 1996

Chief of Naval Operations (CNO) N6 Copernicus: C4ISR for the 21st Century, September 1997

U.S. Marine Corps “...From the Sea” September 1992

Defense Information Systems Agency (DISA): Joint Defense Information Infrastructure Control Center Concept of Operations (DII CC CONOPS); 22 July 1997

Defense Information Systems Agency (DISA); “Defense Information Infrastructure Common Operating Environment (DII COE);” 1 May 1998; http://spider.osfl.disa.mil/dii/ (24 May 1998)

SPAWAR Systems Center San Diego; “Navy C4ISR Technical Architecture” Version 0.9; 17 September 1997.